UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/435,736	11/08/1999	ARTHUR REISMAN	4366-41	5609

48500 7590 03/16/2005

SHERIDAN ROSS P.C.
1560 BROADWAY, SUITE 1200
DENVER, CO 80202

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/435,736	REISMAN, ARTHUR	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) *1,12,15 and 25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-11,13,14,16-24 and 26-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated November 10, 2004 with the amendments to claims 2-4, 6-7, 10, 16-18, 20, 23-24, 26, 28-32 and 33-34, the addition of claims 37-45 and the cancellation of claims 1, 12, 15 and 25.

Response to Arguments

2. Applicant's arguments, filed November 10, 2004, with respect to the rejection(s)of claim(s) 36 under Herr-Hoyman have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Chapman et al. (5,774,650) and Gregg et al. (6,516,416).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 2, 16, 37, 42 and 44-45 are rejected under 35 U.S.C. 102(b) as being anticipated by Chapman et al. (5,774,650).

a) As to claims 44 and 45, Chapman discloses a system and method for controlling access of a plurality users to a computer system over a network comprising at a first computing device (Fig. 2, element 12), receiving input information from a display to a user, the input information comprising at least first (i.e. password) and second datum (i.e. username) corresponding respectively to at least first and second user input fields (col. 5, lines 18-29); at the first computing device, determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user (i.e. the determination is made by encrypting the confidential data, password, and not encrypting non-confidential data, username. This determination also reflects on fig. 2); the first computing device communicating the first datum of the message to a second computing device with encryption of the first datum (col. 5, lines 35-38) and the first computing device communicating the second datum of the message to the second computing device without encryption of the second datum (col. 5, lines 32-34).

b) As to claims 2, 16, 37 and 42, Chapman discloses the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message (col. 5, lines 20-22).

5. Claims 2-7, 10-11, 13-14, 16-20, 23-24, 26-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Gregg et al. (6,516,416).

a) As to claims 36 and 39-40, Gregg discloses a system and method for controlling access to computer resources using an untrusted network (i.e. Internet, Fig. 1) comprising a) providing a display to a user (i.e. user/subscriber interacts with subscription server via the Internet with web browser (col. 2, lines 19-22), the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first (i.e. password) and second (i.e. username) input fields (col. 14, line 66 to col. 15, line 2); b) receiving a message from the user (Fig. 18, element 142), wherein the message comprises at least a first and a second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum (i.e. password) is confidential to the user and the second datum (i.e. username) is non-confidential to the user; c) identifying that the first datum is confidential and the second datum is non-confidential (i.e. acknowledging that password fraud is conducive to fraudulent access and loss of revenue, the effective subscriber authentication is carried out through either a one factor (password) or two factor (password and optional hardware access key with a unique digital ID), col. 1 lines 58-67); d) the first computing device communicating to the second computing device the first datum with encryption (col. 17, lines 32-33) and e) the first computing device communicating to the second computing device the second

datum without encryption (col. 17, lines 30-33) wherein steps (d) and (e) occur at least substantially simultaneously (Fig. 2, element 3).

b) As to claims 44 and 45, Gregg discloses a system and method for controlling access to computer resources using an untrusted network (i.e. Internet, Fig. 1) comprising receiving input information from a display to a user (Fig. 18, element 142), the input information comprising at least first (i.e. password) and second datum (i.e. username) corresponding respectively to at least first and second user input fields (col. 14, line 66 to col. 15, line 2); at the first computing device, determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user (i.e. the determination is made by encrypting the confidential data, password, and not encrypting non-confidential data, username. This determination also reflects on acknowledging that password fraud is conducive to fraudulent access and loss of revenue, the effective subscriber authentication is carried out through either a one factor (password) or two factor (password and optional hardware access key with a unique digital ID), col. 1 lines 58-67); the first computing device communicating the first datum of the message to a second computing device with encryption of the first datum (col. 17, lines 32-33) and the first computing device communicating the second datum of the message to the second computing device without encryption of the second datum (col. 17, lines 30-33).

c) As to claims 2, 16, 37 and 42, Gregg discloses the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message (Fig. 2, element 3).

d) As to claims 3 and 17, Gregg discloses the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message (Fig. 18, element 150; col. 17, lines 42-45).

e) As to claims 4-5, 11, 18-19, 24, 38 and 43, Gregg indicates the same path comprising TCP/IP passage (col. 5, lines 56-61) is used for encrypted and non-encrypted data communications between first computing device and the second computing device. Moreover the system is designed to use the interactive model of the WWW for client server transactions on the Internet (Abstract).

f) As to claims 6, 7 and 20, Gregg shows password and digital ID are encrypted by a key (col. 17, lines 32-34) and the key is communicated from the second computing device to the first computing device (col. 17, lines 32-35).

g) As to claims 10 and 23, Gregg teaches the step of communicating a procedure from the second computing device to the first computing device customer to communicate the encrypted data (col. 17, lines 30-35).

h) As to claims 13-14 and 26-27, Gregg discloses the step for the first computing device to communicate the encrypted and non-encrypted data with the second computing device through the log-in message in which the password is encrypted and username are non-encrypted (Fig. 18, elements 148, 150).

i) As to claim 28, it has the same limitations as claim 44, further the computer readable program code reads on any matter for carrying software.

j) As to claims 29 and 33, Gregg discloses the method wherein the first datum is confidential information to a user [i.e. password (Fig. 18, element 142; element 150)] and the second datum is non-confidential information to the user [i.e. username (Fig. 18, element 142)].

k) As to claims 30 and 34, Gregg discloses the method further comprising:

i) receiving the message from a user, the message comprising a plurality of input fields (i.e. log-in interface with fields for inputting username and password, Fig. 18, element 140).

ii) determining each input field comprising confidential information to the user and each input field comprising non-confidential information to the user, wherein the first datum (i.e. password) is confidential information and the second datum (i.e. username) is non-confidential information (Fig. 18).

l) As to claims 31 and 41, Gregg discloses the method wherein the communicating steps occur at least substantially simultaneously (Fig. 2, element 3).

m) As to claims 32 and 35, Gregg discloses the method wherein the communicating steps comprise:

i) encrypting the information in each of the input fields identified as comprising confidential information (col. 17, lines 32-33).

ii) not encrypting the information in each of the input fields identified as comprising non-confidential information (col. 17, lines 30-33).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 8-9 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gregg et al. (6,516,416) in view of Schneier (Applied cryptography).

Gregg does not disclose a second key is employed to decrypt the first datum of the message and the first and second key comprised a matched key to communicate the encrypted data.

Schneier discloses communications using symmetric cryptography wherein the second key is used to decrypt the encrypted message (page 28, item (5)) and the first

(page 28, item (3)) and second key comprised a matched key (page 28, item (5)) to communicate the encrypted data.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of a second key to decrypt the first datum of the message and the first and second key comprised a matched key to communicate the encrypted data in the system of Gregg, as Schneier teaches so as to protect the sensitive data.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
3/10/05

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER